Office of the Inspector General, DoD

Report No. 9850002R
(Project No. 7OG-9022)

September 1, 1998

Defense Criminal Investigative Organization Programs to Investigate Computer Crimes

Executive Summary

Introduction. We performed this evaluation to determine the current status of the Defense Criminal Investigative Organizations programs to investigate computer crimes.

Evaluation Objectives. The evaluation objectives were to:

o document the programs the Defense Criminal Investigative Organizations (DCIOs) have in place to investigate computer crimes and computer intrusions; and

o identify the resources devoted to the programs.

Evaluation Process. We interviewed DCIO officials at the headquarters offices of DCIOs, reviewed DCIO case summaries, and compiled from DCIO databases statistics that involved computer crimes and computer intrusions.

Evaluation Results.

o The Air Force Office of Special Investigations (AFOSI) established a computer crime investigation program in the 1970s, the Naval Criminal Investigative Service (NCIS) in 1994, and the Army Criminal Investigation Command (USACIDC) and the Defense Criminal Investigative Service (DCIS) in 1998. Only the Air Force presently has real-time capability to detect intrusion in its Service's computer systems. The Air Force computer crimes laboratory is being converted to the Department of Defense computer crimes laboratory, with funding and personnel to be provided by all military Services and DCIS. While the DCIOs have generated investigative results for a number of years in cases that involve theft, damage, and destruction of computer hardware and software, computer intrusion investigations have been less frequently conducted to date, and statistical data is more limited.

o By the end of fiscal year 1998 (FY1998), the DCIOs will average 30 full-time personnel assigned to computer crimes investigations. In addition, all DCIOs have field agents who have received advanced computer training, but who are not assigned full-time to conduct computer crimes investigations. For FY1998, AFOSI and NCIS budgeted or requested over $3 million each in support of their programs. Start-up costs for USACIDC were estimated at $442,000. Training for agents is consistent among the DCIOs and relies heavily on the Federal Law Enforcement Training Center (FLETC) or

DCIOs and relies heavily on the Federal Law Enforcement Training Center (FLETC) or FLETC-equivalent courses for agents, supplemented by other training available from other law enforcement and private industry training sources.

o Competition with the private market makes recruiting and retention of qualified, experienced agents to conduct computer crimes investigations a concern to all the DCIOs. Lack of timely notification of intrusions, inability of the DCIOs to maintain real-time monitoring of Departmental systems, constant training to keep up with technology and hacker activities, funding, and management support within the Department were additional concerns expressed by DCIO management as issues that affect their ability to conduct effective computer intrusion investigations.

Management Comments. Comments received from the Army and Navy are included as Appendix D. All suggestions from the Army were incorporated, and most from the Navy were as well. NCIS provided changes to statistics to Tables 1 and 2 that are different because of the differences in definitions of computer crimes. The statistics reflected in Tables 1 and 2 were derived from the Inspector General's Semiannual Reports to Congress, and were retained to maintain conformance with those previously issued documents.